

FILED ENTERED
LODGED RECEIVED

OCT 25 2018

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

v.

EDWARD KOGAN,
Defendant.

NO. **CR18-258** RSM
INFORMATION

FILED UNDER SEAL

The United States Attorney charges that:

COUNT 1

(Conspiracy to Commit Computer Hacking)

1. The defendant, EDWARD KOGAN, also known as "cooled," and at least five others located abroad committed the successful intrusion of the protected computer network of a victim company, namely, Microsoft Corporation ("Microsoft"). For approximately three weeks beginning in late-January 2017, the cybercriminal group obtained remote access to Microsoft's network, uploaded malicious code, and stole employee credentials and non-public and proprietary files and information owned by Microsoft, including data related to pre-release software and products, which the participants used for their own purposes and, in some cases, published on various online

1 forums and websites. The cybercriminal group did not target, nor compromise, data
2 related to or belonging to customers of Microsoft services.

3 2. Microsoft is a multinational technology company with headquarters in
4 Redmond, Washington. Microsoft develops, manufactures, licenses, supports and sells
5 computer software, consumer electronics, personal computers, and related services. Its
6 best known products include the Microsoft Windows line of operating systems, the
7 Office suite, the Internet Explorer and Edge web browsers, the Xbox video game
8 consoles, and Microsoft Surface personal computers.

9 3. Microsoft's network is a vast and complex web of different computers,
10 servers, and devices. The intrusion in this case targeted the Windows & Devices Group's
11 build services, which are used by developers to produce new software products and
12 updated versions of existing products, such as Windows and Xbox, which have not yet
13 been released to the public. Several of the targeted systems contained portions of
14 software source code that had not been released to the public and were undergoing review
15 by industry partners.

16 4. Source code is highly confidential and valuable intellectual property. For
17 this reason, companies like Microsoft purposely do not release the source code for their
18 products because it would, in effect, allow others to replicate or alter their products.
19 Although no Microsoft customer or partner data was compromised, Microsoft was
20 required to halt the distribution of certain code to ensure no unauthorized modifications
21 had been made.

22 5. By targeting unique servers associated with build services, the group was
23 specifically attempting to gain information on pre-release software builds before their
24 official release for production. For example, one of the main targets for compromise was
25 a legacy externally facing server hosting a support tool called MSSolve. Through the
26 compromise of MSSolve, the cybercriminal group gained access to other servers housing
27 source code of various older versions of Windows. These other servers are used to
28 generate software builds that can be distributed to industry partners for testing within

1 their environments and associated products as part of a quality assurance process. The
2 cybercriminal group also gained entry into servers containing software builds for Xbox-
3 associated software.

4 **I. OFFENSE**

5 6. Beginning at a time unknown, but no later than January 24, 2017, and
6 continuing through on or after March 29, 2017, at Redmond, within the Western District
7 of Washington, and elsewhere, the defendant EDWARD KOGAN, and others known and
8 unknown, did knowingly and willfully combine, conspire, confederate and agree together
9 to commit offenses against the United States, to wit:

10 a. to knowingly cause the transmission of a program, information,
11 code, and command, and as a result of such conduct, intentionally cause damage without
12 authorization to a protected computer, and cause loss to one or more persons during a
13 one-year period aggregating at least \$5,000 in value and damage affecting 10 or more
14 protected computers during a one-year period, in violation of Title 18, United States
15 Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

16 **II. OBJECTIVES OF THE CONSPIRACY**

17 7. The objectives of the conspiracy included hacking into protected computers
18 and servers of Microsoft using deceptive means and malicious software (hereinafter,
19 “malware”) designed to provide the co-conspirators with unauthorized access to non-
20 public data and proprietary information. The objectives of the conspiracy further
21 included locating and exfiltrating files, software, and code, which the conspirators shared
22 with one another and others.

23 **III. MANNER AND MEANS OF THE CONSPIRACY**

24 8. The manner and means used to accomplish the conspiracy included the
25 following:

26 a. The co-conspirators, located in various countries, communicated
27 through messaging applications and Internet Relay Chat (IRC) channels, including one or
28 more chat rooms hosted on a co-conspirator’s private server, called “Ring of Lightning.”

1 Through such means, the co-conspirators coordinated actions and shared information
2 relating to the intrusion of Microsoft's network and the search for and exfiltration of non-
3 public data and proprietary information.

4 b. Through deceptive means, including the use of compromised
5 Microsoft credentials (e.g., username and password) belonging to another person, one or
6 more co-conspirators gained unauthorized remote access to a protected Microsoft
7 computer.

8 c. One or more co-conspirators, using such unauthorized access,
9 identified additional credentials for administrative and employee accounts, which the co-
10 conspirators used to move laterally throughout Microsoft's network, compromising
11 additional computers and servers, many of which were located in the Western District of
12 Washington. The group largely targeted computers and servers used by software
13 developers to share and store Microsoft products, some of which were still in the pre-
14 release and development stages and, in some cases, were never released publicly.

15 d. One or more co-conspirators implanted multiple types of code on
16 Microsoft's network. For example, one of the types of malicious code included a "web
17 shell" that provided a platform for the co-conspirators to access Microsoft's network and
18 to search the Microsoft file repository for particular files of interest and download
19 selected files. This "web shell" also allowed the co-conspirators to interact directly with
20 the compromised system and execute standard Windows system commands to view
21 processes, services, and perform system administration tasks. Another type of program
22 that a co-conspirator uploaded allowed users to scan the network for servers listening on
23 particular "ports" and potentially to look for specific vulnerabilities. The co-conspirator
24 also compromised Microsoft employee account credentials and "service account"
25 credentials. These credentials were required to facilitate the conspiracy's use of the "web
26 shell" and to move within Microsoft's protected network.

27 e. The co-conspirators, including EDWARD KOGAN, without
28 authorization, accessed Microsoft's protected system and ran tens of thousands of

1 individual queries for files and information across Microsoft's network. Search terms
2 included, among other things, Microsoft-specific terms and internal codenames for pre-
3 release products, demonstrating a heightened level of sophistication and familiarity with
4 Microsoft's business processes.

5 f. The co-conspirators, including EDWARD KOGAN, downloaded
6 without authorization more than 5,000 files from Microsoft's network. This included
7 non-public data and proprietary information related to Microsoft internal policies as well
8 as Microsoft products, including source code for pre-release software builds, Windows
9 operating systems, and Microsoft Xbox games consoles.

10 g. The co-conspirators, including EDWARD KOGAN, shared
11 information with one another and used the unauthorized network access and stolen
12 Microsoft information for their own use and benefit. For instance, the co-conspirators
13 gathered many non-public files and placed copies on one or more shared servers,
14 accessible to the members of the conspiracy and others, associated with a particular
15 website, owned and maintained by a member of the conspiracy, specifically dedicated to
16 monitoring and tracking Microsoft product updates.

17 **IV. OVERT ACTS**

18 9. In furtherance of the conspiracy, and to achieve the objects thereof, the
19 defendant, and others known and unknown, did commit and cause to be committed, the
20 following overt acts, among others, in the Western District of Washington and elsewhere:

21 a. On or about January 24, 2017, a co-conspirator located in the United
22 Kingdom (UK), also known as "Rai-chan" (hereinafter "Co-Conspirator #1"), used
23 compromised credentials to gain unauthorized remote access to a protected Microsoft
24 computer.

25 b. On or about January 24, 2017, Co-Conspirator #1 uploaded various
26 malicious code to a protected Microsoft computer, which damaged the integrity of the
27 data, a program, a system, and information stored thereon. Similar malware uploads
28 occurred on various dates thereafter.

1 c. On or about January 27, 2017, Co-Conspirator #1 conducted queries
2 for particular files and information. Co-Conspirator #1 conducted similar searches and
3 exfiltrated files from Microsoft servers on various dates thereafter.

4 d. On or about January 28, 2017, in an IRC chat room dedicated to the
5 targeting of Microsoft's networks, Co-Conspirator #1 shared with others the link to the
6 "web shell" providing access to Microsoft's network, along with the message "got api
7 [application programming interface] ready."

8 e. On or about January 28, 2017, a co-conspirator located in the United
9 Arab Emirates (UAE), also known as "Airportsfan" (hereinafter "Co-Conspirator #2"),
10 accessed Microsoft's network through the platform created by the malware and
11 conducted queries for particular files and information. Co-Conspirator #2 conducted
12 similar searches and exfiltrated files from Microsoft servers on various dates thereafter.

13 f. On or about January 28, 2017, a co-conspirator located in Eastern
14 Europe, specifically, Slovakia, also known as "lucascor" (hereinafter "Co-Conspirator
15 #3"), accessed Microsoft's network through the platform created by the malware and
16 conducted queries for particular files and information. Co-Conspirator #3 conducted
17 similar searches and exfiltrated files from Microsoft servers on various dates thereafter.

18 g. On or about February 2, 2017, EDWARD KOGAN, located in the
19 United States, specifically, the state of Florida, using a proxy Internet Protocol (IP)
20 address in New York, accessed Microsoft's network through the platform created by the
21 malware and conducted queries for particular files and information. EDWARD KOGAN
22 conducted similar searches and exfiltrated files from Microsoft servers on various dates
23 thereafter.

24 h. On or about February 2, 2017, a co-conspirator located in Western
25 Europe, specifically, the Netherlands, also known as "ultrawindows" (hereinafter "Co-
26 Conspirator #4"), accessed Microsoft's network through the platform created by the
27 malware and conducted queries for particular files and information. Co-Conspirator #4
28

1 conducted similar searches and exfiltrated files from Microsoft servers on various dates
2 thereafter.

3 i. On or about February 8, 2017, in an IRC chat room, various co-
4 conspirators, including EDWARD KOGAN, discussed Microsoft internal training
5 materials, discovered on Microsoft's network, related to the handling and storage of
6 "sensitive" company information.

7 j. On various dates, EDWARD KOGAN and his co-conspirators
8 shared information and coordinated their efforts to locate items of interest on Microsoft's
9 network. By way of example,

10 i. On February 2, 2017, EDWARD KOGAN ran queries for a
11 particular Microsoft software build, identified by unique number. Shortly thereafter, also
12 on February 2, 2017, the Twitter account for the website owned and maintained by a co-
13 conspirator located in the UK, also known as "hounsell" (hereinafter "Co-Conspirator
14 #5"), announced (tweeted) that the new Microsoft build had been published on the
15 website. Minutes later, Co-Conspirator #5 posted on his personal Twitter account a link
16 to (retweeted) the website's Twitter announcement, along with the comment, "mm, looks
17 like we're back in business on [website], that winter turbulence is (hopefully) over."

18 ii. On February 2, 2017, in an IRC chat room, various co-
19 conspirators, including EDWARD KOGAN, discussed searching for files relating to the
20 Xbox video game console. EDWARD KOGAN expressed his belief to his co-
21 conspirators that files and information about a specific version of the Xbox video game
22 console "should be here." In doing so, EDWARD KOGAN referred to the device by its
23 internal Microsoft codename.

24 iii. On February 11, 2017, in an IRC chat room, various co-
25 conspirators, including EDWARD KOGAN, discussed the exfiltration of files and
26 information related to the Xbox video game console. As part of the dialogue, EDWARD
27 KOGAN suggested to a co-conspirator, "...you should look for the xbox signing tools."
28

1 k. On or about February 16, 2017, having detected the intrusion and
2 having conducted an extensive internal investigation and remediation effort, Microsoft
3 successfully terminated the cybercriminal group's unauthorized access to Microsoft's
4 network. On the same date, and thereafter, co-conspirators discussed changes to the
5 passwords for accounts they were using to access Microsoft's network and the need to
6 locate and acquire new passwords to re-establish and maintain unauthorized access to the
7 protected system.

8 l. On or about March 29, 2017, one or more co-conspirators regained
9 unauthorized remote access to a protected Microsoft computer. Microsoft detected the
10 intrusion and again successfully terminated the unauthorized access to Microsoft's
11 network.

12 10. The offense conduct, summarized above, caused direct and foreseeable
13 harm to Microsoft, in the Western District of Washington and elsewhere, including the
14 theft of more than 5,000 internal files, which included source code and other non-public
15 data and proprietary information about Microsoft and its various products, and damage to
16 over 30 protected computers, each of which was used in and affected interstate and
17 foreign commerce and communication. The total monetary harm caused to Microsoft by
18 the intrusion remains under investigation. The internal investigation and remediation
19 costs alone exceed \$1,000,000.

20 All in violation of Title 18, United States Code, Section 371.

21
22 **FORFEITURE ALLEGATION**

23 11. The allegations contained in Count 1 of this information are hereby
24 realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to
25 Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i). Upon conviction of the
26 offense charged in Count 1, the defendant shall forfeit to the United States any property
27 constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as
28 the result of such offenses, and shall also forfeit the defendant's interest in any personal

1 property that was used or intended to be used to commit or to facilitate the commission of
2 such offense.

3 12. If any of the property described above, as a result of any act or omission of
4 the defendant:

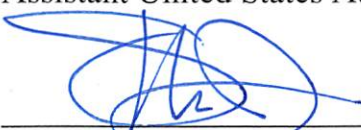
- 5 a. cannot be located upon the exercise of due diligence;
6 b. has been transferred or sold to, or deposited with, a third party;
7 c. has been placed beyond the jurisdiction of the court;
8 d. has been substantially diminished in value; or
9 e. has been commingled with other property which cannot be divided
10 without difficulty,

11 the United States of America shall be entitled to forfeiture of substitute property pursuant
12 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
13 Code, Section 2461(c).

14
15 DATED this 25th day of October, 2018.

16
17 
18 ANNETTE L. HAYES
19 United States Attorney

20
21 
22 ANDREW C. FRIEDMAN
23 Assistant United States Attorney

24
25 
26 STEVEN T. MASADA
27 Assistant United States Attorney
28